CYBER SECURITY CHECKLIST

PHYSICAL SECURITY	YES	NO
1. Is your computing area and equipment physically secured?		
2. Are there procedures in place to prevent terminals from being left in a logged-on state, however briefly?		
3. Are screens automatically locked after 10 minutes idle?		
4. Are modems set to Auto-Answer OFF (not to accept incoming calls)?		
5. Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)?		
6. Does your staff wear ID badges?		
7. Do you check the credentials of external contractors?		
8. Do you have procedures for protecting data during equ8pment repairs?		
9. Is waste paper binned or shredded?		
10. Do you have procedures for disposing of waste material?		
11. Do your policies for disposing of old computer equipment protect against loss of date (e.g.. by reading old disks and hard drives)?		
12. Do you have policies covering laptop security (e.g. cable lock or secure storage)?		
ACCOUNT AND PASSWORD MANAGEMENT	**YES**	**NO**
13. Do you ensure that only authorized personnel have access to your computers?		
14. Do you require and enforce appropriate passwords?		
15. Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?		
16. Are you computers set up so others cannot view staff entering passwords?		

CONFIDENTIALITY OF SENSITIVE DATA	YES	NO
17. Are you exercising responsibilities to protect sensitive data under your control? 18. Is the most valuable or sensitive data encrypted?		
DISASTER RECOVERY	**YES**	**NO**
19. Do you have a current business continuity plan?		
SECURITY AWARENESS AND EDUCATION	**YES**	**NO**
20. Are you providing information about computer security to your staff? 21. Are employees taught to be alert to possible security breaches?		

CYBER SECURITY THREAT ASSESSMENT

This is an example of a threat checklist using 0-5 rating scales for impact and probability

IMPACT SCALE	PROBABILITY SCALE
1. Impact is negligible	0. Unlikely to occur
2. Effect is minor, major agency operations are not affected	1. Likely to occur less than once per year
3. Agency operations are unavailable for a certain amount of time, costs are incurred. Public/customer confidence is minimally affected	2. Likely to occur once per year
4. Significant loss of operations, significant impact on pubic/customer confidence	3. Likely to occur once per month
5. Effect is disastrous, systems are down for an extended period of time, systems need to be rebuilt and data replaced	4. Likely to occur once per week
6. Effect is catastrophic, critical systems are offline for an extended period; data are lost or irreparably corrupted; public health and safety are affected	5. Likely to occur daily

GENERAL THREATS	**Impact (0-5)**	**Probability (0-5)**	**Total (Impact x Probability)**
Human Error: 1. Accidental destruction, modification, disclosure, or incorrect classification of information 2. Ignorance: inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge 3. Workload: Too many or too few system administrators, highly pressured users 4. Users may inadvertently give information on security weaknesses to attackers 5. Incorrect system configuration 6. Security policy not adequate 7. Security policy not enforced 8. Security analysis may have omitted something important or be wrong.			
THREATS	**Impact (0-5)**	**Probability (0-5)**	**Total (Impact x Probability)**
1. Dishonesty: Fraud, theft, embezzlement, selling of confidential agency information 2. Attacks by "social engineering" ● Attackers may use telephone to impersonate employees to persuade users/administrators to give user name/passwords/modem numbers, etc. ● Attackers may persuade users to execute Trojan Horse programs 3. Abuse of privileges/trust			

4. Unauthorized use of "open" terminals/PC' 5. Mixing of test and production data or environments 6. Introduction of unauthorized software or hardware 7. Time bombs: Software programmed to damage a system on a certain date 8. Operating system design errors: Certain systems were not designed to be highly secure 9. Protocol design errors: Certain protocols were not designed to be highly secure. Protocol weaknesses in TCP/IP can result in: ● Source routing, DNS spoofing, TCP sequence guessing, unauthorized access ● Hijacked sessions and authentication session/transaction replay, data is changed or copied during transmission ● Denial of service, due to ICMP bombing, TCP-SYN flooding, large PING packets, etc. 10. Logic bomb: Software programmed to damage a system under certain conditions 11. Viruses in programs, documents, e-mail attachments			
IDENTIFICATION AUTHORIZATION THREATS	**Impact (0-5)**	**Probability (0-5)**	**Total (Impact x Probability)**
1. Attack programs masquerading as normal programs (Trojan horses). 2. Attack hardware masquerading as normal commercial hardware			

3. External attackers masquerading as valid users or customers 4. Internal attackers masquerading as valid users or customers 5. Attackers masquerading as help desk/support personnel			
PRIVACY THREATS	**Impact (0-5)**	**Probability (0-5)**	**Total (Impact x Probability)**
1. Eavesdropping ● Electromagnetic eavesdropping / Ban Eck radiation ● Telephone/fax eavesdropping (via "clip-on" telephone bugs, inductive sensors, or hacking the public telephone exchanges ● Network eavesdropping. Unauthorized monitoring of sensitive data crossing the internal network, unknown to the data owner ● Subversion of ONS to redirect email or other traffic ● Subversion of routing protocols to redirect email or other traffic ● Radio signal eavesdropping, 2. Rubbish eavesdropping (analyzing waste for confidential documents, etc.)			

INTEGRITY / ACCURACY THREATS	**Impact (0-5))**	**Probability (0-5)**	**Total (Impact x Probability)**
1. Malicious, deliberate damage of information or information processing functions from external sources 2. Deliberate modification of information			
ACCESS CONTROL THREATS	**Impact (0-5)**	**Probability (0-5)**	**Total Impact x Probability)**
1. Password cracking (access to password files, use of bad – blank, default, rarely changed – passwords) 2. External access to password files, and sniffing of the networks 3. Attack programs allowing external access to systems (back doors visible to external networks) 4. Attack programs allowing internal access to systems (back doors visible to internal networks) 5. Unsecured maintenance modes, developer back doors 6. Modems easily connected, allowing uncontrollable extension of the internal network 7. Bugs in network soft are which can open unknown/unexpected security holes (holes can be exploited from external networks to gain access. This threat grows as software becomes increasingly complex) 8. Unauthorized physical access to system			

REPUDIATION THREAT	**Impact (0-5))**	**Probability (0-5**	**Total (Impact x Probability)**
1. Receivers of confidential information may refuse to acknowledge receipt 2. Senders of confidential information may refuse to acknowledge source			
LEGAL THREATS	**Impact (0-5)**	**Probability (0-5)**	**Total (Impact x Probability)**
1. Failure to comply with regulatory or legal requirements (ie, to protect confidentiality of employee data) 2. Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (ie, incitement to racism, gambling, money laundering, distribution of pornographic or violent material) 3. Liability for damages if an internal user attacks other sites.			
RELIABILITY OF SERVICE THREATS	**Impact (0-5)**	**Probability (0-5)**	**Total (Impact x Probability)**
1. Major natural disasters, fire, smoke, water, earthquake, storms/hurricanes/tornadoes, power outages, etc 2. Minor natural disasters, of short duration, or causing little damage 3. Major human-caused disasters: war, terrorist incidents, bombs, civil disturbance, dangerous chemicals, radiological accidents, etc. 4. Equipment failure from defective hardware, cabling, or communications system. 5. Equipment failure from airborne dust, electromagnetic interference, or static electricity			

6 Denial of Service: ● Network abuse: Misuse of routing protocols to confuse and mislead systems ● Server overloading (processes, swap space, memory, "tmp" directories, overloading services) ● Email bombing Downloading or receipt of malicious Applets, Active X controls, macros, PostScript files, etc. 7. Sabotage: Malicious, deliberate damage of information or information processing functions ● Physical destruction of network interface devices, cables ● Physical destruction of computing devices or media ● Destruction of electronic devices and media by electromagnetic radiation weapons (HERF Gun, EMP/T Gun) ● Deliberate electrical overloads or shutting off electrical power ● Viruses and/or worms. Deletion of critical systems files			